50272-101

REPORT DOCUMENTATION PAGE	1. REPORT NO. DCA/SW/MT-88/0010	2.	3. Recipient's Accession No.
4. Title and Subtitle: Defense Communications Agency Upper Level Protocol Test System Internet Protocol Security Option Test Traceability Index			5. Report Date: May 1988
			6.
7. Author(s)			8. Performing Organization Rept. No.
9. Performing Organization Name and Address: Defense Communications Agency, Defense Communications Engineering Center, Code R640, 1860 Wiehle Ave., Reston, VA 22090-5500			10. Project/Task/Work Unit No.
			11. Contract(C) or Grant(G) No. (C) (G)
12. Sponsoring Organization Name and Address			13. Type of Report & Period Covered: FINAL
			14.

15. Supplementary Notes

For magnetic tape, see: ADA195128

16. Abstract (Limit: 200 words)

This document is part of a software package that provides the capability to conformance test the Department of Defense suite of upper level protocols including: Internet Protocol (IP) Mil-Std 1777, Transmission Control Protocol (TCP) Mil-Std 1778, File Transfer Protocol (FTP) Mil-Std 1780, Simple Mail Transfer Protocol (SMTP) Mil-Std 1781 and TELNET Protocol Mil-Std 1782.

See p 1

17. Document Analysis a. Descriptors

Protocol Test Systems
Conformance Testing
Department of Defense Protocol Suite

b. Identifiers/Open-Ended Terms

Internet Protocol (IP)
Transmission Control Protocol (TCP)
File Transfer Protocol (FTP)
Simple Mail Transfer Protocol (SMTP)
TELNET Protocol

c. COSATI Field/Group

18. Availability Statement	19. Security Class (This Report)	21. No. of Pages
Unlimited Release	UNCLASSIFIED	7
	20. Security Class (This Page) UNCLASSIFIED	22. Price

DEFENSE COMMUNICATIONS AGENCY

UPPER LEVEL PROTOCOL TEST SYSTEM

INTERNET PROTOCOL SECURITY OPTION TEST TRACEABILITY INDEX

MAY 1988

Disclaimer Concerning Warranty and Liability

This software product and documentation and all future updates to it are provided by the United States Government and the Defense Communications Agency (DCA) for the intended purpose of conducting conformance tests for the DoD suite of higher level protocols. DCA has performed a review and analysis of the product along with tests aimed at insuring the quality of the product, but does not warranty or make any claim as to the quality of this product. The product is provided "as is" without warranty of any kind, either expressed or implied. The user and any potential third parties accept the entire risk for the use, selection, quality, results, and performance of the product and updates. Should the product or updates prove to be defective, inadequate to perform the required tasks, or misrepresented, the resultant damage and any liability or expenses incurred as a result thereof must be borne by the user and/or any third parties involved, but not by the United States Government, including the Department of Commerce and/or The Defense Communications Agency and/or any of their employees or contractors.

Distribution and Copyright

Comments

Comments or questions about this software product and documentation can be addressed in writing to:

DCA Code R640
1860 Wiehle Ave
Reston, VA 22090-5500
ATTN: Protocol Test System Administrator

INTERNET PROTOCOL SECURITY OPTION (IPSO)
MIL-STD-1777 DRAFT REVISION
TRACEABILITY MATRIX

This Traceability Matrix provides information on the derivation, organization, and function of tests specified for IPSO within the Protocol Test system.

The document is divided into four sections:

IPSO TRACEABILITY INDEX;
IPSO TEST INDEX;
IPSO TEST SCENARIOS INDEX;
IPSO SCENARIOS AND TESTS DESCRIPTIONS.

IPSO TRACEABILITY INDEX: IPSO TEST NUMBERS VERSUS IP MIL-STD-1777 SECURITY OPTION . . .

The table indicates the cross-reference between the Test Scenarios and the applicable section in MIL-STD-1777 and the BLACKER BFE ICD regarding each required function, operation, option, mode, response, or state.

IPSO TEST INDEX: IPSO TEST NUMBERS VERSUS THE SECURITY REQUIREMENT . . .

The table shows the IP Test Numbers that may be regarded as the "principle test" for each requirement of the IPSO.

IPSO TEST SCENARIOS INDEX: IPSO TEST SCENARIO FILES VERSUS IPSO TEST NUMBERS . . .

The table shows, for each IPSO Test Number, the UNIX file names of the IPSO Test Scenario Files in which that number appears.

IPSO SCENARIOS AND TESTS DESCRIPTIONS . . .

This section provides a brief narrative of the scope and objectives of each IPSO Test Scenario File and an operational description of each IPSO Test Number.

==========

SECTION 1 - IPSO TRACEABILITY INDEX

IPSO Test Numbers Versus IP MIL-STD-1777 Reference Draft Revised IP Security Option or Blacker BFE ICD (March 6, 1985).

The table indicates the cross-reference between the IPSO tests and the applicable sections of either the Draft Revised Mil-Std-1777 or the Blacker BFE ICD.

Reference		Test Number
Draft Revised IP Security Option		
9.3.15.3	DoD Basic Security	1, 2, 4
9.3.15.3.1	DoD Basic Security Length	2
9.3.15.3.2	Class. Protection Level	1, 5
9.3.15.3.3	Protection Authorities	1, 6, 7
9.3.15.3.4	Usage Rules	1, 5, 7
9.3.15.4	Extended Security Option	3

SECTION 2 - IPSO TEST INDEX

IPSO Test Numbers Versus the Security Requirement.

The table shows the IPSO Test Numbers that may be regarded as the "principle tests" for each requirement on IP security.

Test Number	Purpose
1	Basic Security Option and Accreditation Validation
2	Basic Security Option Detection and Syntax Validation
3	Extended Security Option Detection and Syntax Validation
4	Correct Security Labeling in All Fragments
5	Correct Security Usage
6	Correct Accreditation Usage
7	Variable Length Accreditation Mask

==========

SECTION 3 - IPSO TEST SCENARIOS INDEX

IPSO Test Scenario Files Versus IPSO Test Numbers.

Test Number	Scenario Name
1	IPSO
2	IPSO
3	IPSO
4	IPSO
5	IPSO
6	IPSO
7	IPSO

SECTION 4 - IPSO SCENARIOS AND TESTS DESCRIPTIONS

This section provides a brief narrative of the scope and objectives of each IPSO Test Scenario File and a narrative of each individual test in that scenario.

==========

Scenario IPSO

Scenario IPSO evaluates an IUT's general conformance to the Draft IPSO Addendum of Mil-Std-1777 on IP Security. Scenario IPSO will validate the presence of fields and the correctness of the syntax in the option.

Test 1: BASIC SECURITY OPTION AND ACCREDITATION VALIDATION

The IUT should accept only IP datagrams with the single classification for which it has been accredited. The accreditation agency is denoted by the accreditation mask accompanying the classification parameter. Therefore, the classification and accreditation mask on system-high hosts form a unique filter for incoming IP datagrams. Also, multilevel secure hosts can only have a single classification for a given line, so the same test will work for multilevel hosts on a line-by-line test basis.

- Action: The Central Driver will send all possible combinations of classification; and accreditations mask and record the response to each request.
- Verification: Only one datagram should reach the Remote Driver, and that one should be echoed back.
- Success: One IP datagram is generated by the IUT with the IUT's accredited classification.
- Failure: None of the datagrams generate a response.

Test 2: BASIC SECURITY OPTION DETECTION AND SYNTAX VALIDATION

Does the IUT send only one Basic Security Option (BSO) per IP Datagram (i.e., option type 130)? Is the format of that packet correct?

- Action: Remote Driver returns an IP datagram with the security option specified correctly.

- Verification:

    - Option type = 130 decimal.
    - Length is consistent with option length.
    - Classification should be identical with packet sent from reference.
    - Authority flags set equal to specified codes.
    - Only one option type 130 is present.

- Success: All of the verification criteria are met.

- Failure: Either a verification criterion is incorrect or more than one option type 130 is located.

Test 3: EXTENDED SECURITY OPTION DETECTION AND SYNTAX VALIDATION

If the IUT's datagram contains an extended security option (option type 133), is the format of the packet correct?

- Action: Remote Driver returns an IP datagram with the extended security option specified.

- Verification: Option type = 133 decimal.

- Success: Option is located.

- Failure: Not applicable.

Test 4: CORRECT SECURITY LABELING OF ALL FRAGMENTS

If the IUT fragments an IP datagram, it must place the Basic Security Option (BSO) in all packets.

- Action: Remote Driver is requested to send continuously larger data segments in an effort to force the IP IUT to fragment the datagram.

- Verification: Basic option type 130 must be located in all fragments with a consistent specification for the security.

- Success: All fragments contain the BSO and all fragments have the same level.

- Failure: A fragment that is found without the BSO or the value of the classification is not consistent.

TEST 5: CORRECT SECURITY USAGE

Continuously increase the security classification of IP datagrams that the Remote Driver is asked to set in the echo packet.

- Action: Central Driver will send valid IP datagrams requesting the Remote Driver to generate IP datagrams with increasing security classification. The accreditation authority will be held constant.

- Verification: The Central Driver will log the classification setting and the result from the IUT.

- Success: Only datagrams with the accredited security classification should be returned.

- Failure: Datagrams at different security levels are returned.

TEST 6: CORRECT ACCREDITATION USAGE

The IUT IP should send datagrams with only one accreditation mask.

- Action: A series of datagrams are sent to the IUT's Remote Driver requesting that the accreditation mask be set to a different but valid combination in each datagram. Each datagram will contain an IP Remote Driver command to echo back the datagram.

- Verification: The Central Driver will log the accreditation mask that is sent and the response, if received.

- Success: Only one accreditation mask will be received.

- Failure: Different accreditation masks are received.

TEST 7: MULTIPLE LENGTH ACCREDITATION MASK

The IPSO Addendum allows for a multi-octet-length Accreditation mask, even though it specifies only a single octet at the present time. This test will observe the IUT's handling of a multi-octet accreditation option.

- Action: The reference will send a valid IP datagram with a multi-octet accreditation field. The field will be syntactically correct, specifying only the proper accreditation entities. A second datagram will be sent with a multi-octet accreditation field that is syntactically incorrect. Again, the Remote Driver will be asked to echo back the datagram.

Verification: The reference should receive and log the datagram's echo.

Success: A receipt of an echo for the first datagram.

Failure: A receipt of an echo for the second datagram.